



1919 Pennsylvania Avenue NW  
Suite 800  
Washington, DC 20006-3401

**Paul B. Hudson**  
202.973.4275 tel  
202.973.4499 fax  
paulhudson@dwt.com

February 6, 2014

**VIA ELECTRONIC FILING**

Marlene H. Dortch  
Office of the Secretary  
Federal Communications Commission  
445 12th Street, S.W.  
Washington, D. C. 20554

Re: EB Docket 06-36, Annual 47 C.F.R. § 64.2009(e) CPNI Certification

Dear Ms. Dortch:

Pursuant to Section 64.2009(e) of the Commission's rules, 47 C.F.R. § 64.2009(e), enclosed for filing in the above-referenced docket is the executed annual CPNI Compliance Certificate of Pacific Telecom Services, Inc. Attached to the certificate is a summary of the company's CPNI policies and procedures.

Respectfully submitted,

A handwritten signature in black ink, appearing to read 'P. Hudson'.

Paul B. Hudson  
Counsel for Pacific Telecom Services, Inc.

Encl.

Annual 47 C.F.R. § 64.2009(e) CPNI Certification

EB Docket 06-36

Annual 64.2009(e) CPNI Certification for 2014 covering the prior calendar year 2013

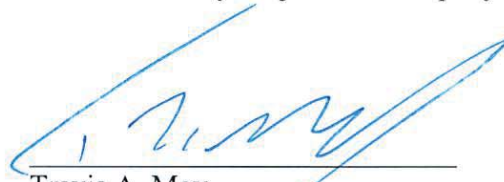
1. Date filed: February 6, 2014
2. Name of company covered by this certification: Pacific Telecom Services, Inc.
3. Form 499 Filer ID: 823794
4. Name of signatory: Travis A. May
5. Title of signatory: President
6. Certification:

I, Travis A. May, certify that I am President of Pacific Telecom Services, Inc. ("Company"), and, acting as an agent of the Company, that I have personal knowledge that the Company has established operating procedures, as summarized in the attached statement, that are adequate to ensure compliance with the Commission's customer proprietary network information ("CPNI") rules as set forth in Part 64, Subpart U of the Commission's rules, 47 C.F.R. §§ 64.2001 *et seq.*

Attached to this certification is an accompanying statement explaining how the Company's procedures ensure that the Company is in compliance with the requirements (including those mandating the adoption of CPNI procedures, training, recordkeeping, and supervisory review) set forth in section 64.2001 *et seq.* of the Commission's rules.

The Company has not received any customer complaints in the past calendar year concerning unauthorized release of CPNI. The Company does not have any material information with respect to the processes pretexters are using to attempt to access CPNI that is not already a part of the record in the Commission's CC Docket No. 96-115. The Company has therefore not taken any actions in the past year against data brokers, including proceedings instituted or petitions filed by the company at either state commissions, the court system or at the Commission.

I hereby represent and warrant that the above certification is consistent with Section 1.17 of the Commission's rules, 47 C.F.R. § 1.17, which requires truthful and accurate statements to the Commission, and acknowledge that false statements and misrepresentations to the Commission are punishable under Title 18 of the U.S. Code and may subject the Company to enforcement actions.

  
\_\_\_\_\_  
Travis A. May  
President  
Pacific Telecom Services, Inc.  
Executed 4 Feb, 2014

## **CPNI Compliance Policies of Pacific Telecom Services, Inc.**

Pacific Telecom Services, Inc. (“PTS”) has implemented the following policies and procedures to protect the confidentiality of Customer Proprietary Network Information (“CPNI”) and to assure compliance with the rules of the Federal Communications Commission (“FCC”) set forth in 47 C.F.R. Part 64, Subpart U, Section 2001 *et seq.*, as revised by the FCC’s new rules adopted in *Implementation of the Telecommunications Act of 1996: Telecommunications Carriers’ Use of Customer Proprietary Network Information and Other Customer Information*, CC Docket No. 96-115, Report and Order and Further Notice of Proposed Rulemaking, FCC 07-22 (rel. April 2, 2007). PTS’ policy is administered by its CPNI Compliance Officer, Michael Haley.

CPNI is “(A) information that relates to the quantity, technical configuration, type, destination, location, and amount of use of a telecommunications service subscribed to by any customer of a telecommunications carrier, and that is made available to the carrier by the customer solely by virtue of the carrier-customer relationship; and (B) information contained in the bills pertaining to telephone exchange service or telephone toll service received by a customer of a carrier.”

### **I. USE, DISCLOSURE OF, AND ACCESS TO CPNI**

PTS is exclusively a wholesale service provider that offers wholesale origination and termination services to other telecommunications service providers, primarily to customers located outside of the United States. PTS therefore does not provide telecommunications services to any end user consumers in the United States. In accordance with Section 222(b) of the Act, 47 U.S.C. § 222(b), when PTS receives or obtains proprietary information from a carrier for purposes of providing a telecommunications service, it only uses such information for such purpose. PTS does not use such information or any other CPNI for any marketing of any kind.

PTS may use, disclose, or permit access to CPNI only in its provision of the communications service from which such information is derived; for services necessary to, or used in, the provision of such communications service, including activities to initiate, render, bill and collect for telecommunications services; to protect the rights or property of PTS, or to protect users or other carriers or service providers from fraudulent, abusive or unlawful use of, or subscription to, such services; to provide installation, maintenance, or repair services; as required by law; or as expressly authorized by the customer.

PTS does not use, disclose or permit access to CPNI to identify or track customers that call competing service providers.

### **II. SAFEGUARDS AGAINST DISCLOSURE OF CPNI TO UNAUTHORIZED PARTIES**

Pursuant to 47 C.F.R. § 64.2010(g), the FCC’s authentication requirements set forth in § 64.2010 do not apply to PTS’ customers, because all such customers are business customers who may contact a dedicated account representative, and all have a contract with PTS that specifically addresses the protection of CPNI and other confidential information. In any event, PTS does not disclose Call Detail Information or other CPNI to any inbound telephone caller and does not

provide CPNI to any visitor to a retail office that has not been properly authenticated. PTS provides a web site that can be accessed by its wholesale customers to access information related to their account. PTS employs security measures to authenticate users of this website that are in accordance with the customer contracts described herein.

When a customer address of record is created or changed, PTS will send a notice to a preexisting customer address of record notifying it of the change. This notice requirement does not apply when the customer initiates service. The notices will not reveal the changed information and will direct the customer to notify PTS immediately if it did not authorize the change. There are no passwords, customer response to a back-up means of authentication for lost or forgotten passwords, or online accounts associated with CPNI possessed by PTS that are subject to the FCC's CPNI authentication rules.

Above and beyond the specific FCC requirements, PTS will take reasonable measures to discover and protect against attempts to gain unauthorized access to CPNI. The FCC's rules require carriers on an ongoing basis to "take reasonable measures to discover and protect against activity that is indicative of pretexting." If any employee becomes aware of new methods that are being used or could be used by third parties to attempt to obtain unauthorized access to CPNI, or of possible changes to PTS' existing policies that would strengthen protection of CPNI, they should report such information immediately to PTS' CPNI Compliance Officer so that PTS may evaluate whether existing policies should be supplemented or changed.

### **III. REPORTING CPNI BREACHES TO LAW ENFORCEMENT**

Any PTS employee that becomes aware of any breaches, suspected breaches or attempted breaches of CPNI must report such information immediately to the PTS CPNI Compliance Officer, and must not report or disclose such information by any employee to any non-employee, including the potentially affected customer, except in express conformance with the procedures described below. Any employee that fails to report such information will be subject to disciplinary action that may include termination.

It is PTS' policy that employees should not be discouraged from reporting information about breaches that may have been caused in part by their own actions or omissions. Once a breach has occurred, the most important objective is to attempt to limit the damage to customers, make any adjustments as needed to prevent a recurrence of the breach, and to alert law enforcement promptly. Therefore, although employees who violate PTS' CPNI compliance policies are subject to discipline, the sanctions may be substantially reduced where employees promptly self-report violations if appropriate.

#### **A. Identifying a "Breach"**

A "breach" has occurred when any person, without authorization or exceeding authorization, has intentionally gained access to, used, or disclosed CPNI. If an employee has information about an incident and is not certain that the incident would not constitute a breach under this definition, the incident must be reported to the CPNI Compliance Officer.

If a PTS employee determines that an unauthorized person is attempting to gain access to CPNI but does not succeed at doing so, no breach has occurred. However, the incident must be reported to PTS' CPNI Compliance Officer who will determine whether to report the incident to law enforcement and/or take other appropriate action. PTS' Compliance Officer will determine whether it is appropriate to update PTS' CPNI policies or training materials in light of any new information; the FCC's rules require PTS on an ongoing basis to "take reasonable measures to discover and protect against activity that is indicative of pretexting."

## **B. Notification Procedures**

As soon as practicable, and in no event later than seven (7) business days upon learning of a breach, the PTS CPNI Compliance Officer shall electronically notify the United States Secret Service (USSS) and the Federal Bureau of Investigation (FBI) by accessing the following link: <https://www.cpnireporting.gov>. PTS' FRN number and password may be required to submit a report. If this link is not responsive, the PTS CPNI Compliance Officer will contact counsel or the FCC's Enforcement Bureau (202-418-7450 or <http://www.fcc.gov/eb/cpni>) for instructions.

Except as provided below, PTS will not notify customers or disclose a breach to the public until 7 full business days have passed after notification to the USSS and the FBI. (A full business day does not count a business day on which the notice was provided.) Federal law requires compliance with this requirement even if state law requires disclosure.

If PTS receives no response from law enforcement after the 7<sup>th</sup> full business day, it must promptly proceed to inform the customers whose CPNI was disclosed of the breach. PTS will delay notification to customers or the public upon request of the FBI or USSS. If the PTS Compliance Officer believes there is a need to disclose a breach sooner, he or she should so indicate in the notification to law enforcement. However, such notification does not itself permit notice to customers; PTS still may not notify customers sooner unless given clearance to do so from both the USSS and the FBI.

## **IV. RECORD RETENTION**

The CPNI Compliance Officer is responsible for assuring that PTS maintains for at least two years a record, electronically or in some other manner, of any breaches discovered, notifications made to the USSS and the FBI pursuant to these procedures, and notifications of breaches made to customers. The record must include, if available, dates of discovery and notification, a detailed description of the CPNI that was the subject of the breach, and the circumstances of the breach.

PTS maintains a record, for a period of at least one year, of those limited circumstances in which CPNI is disclosed or provided to third parties, or where third parties were allowed access to CPNI.

Because PTS does not use CPNI for marketing or for any other purpose for which customer approval is required, it does not have any records regarding: supervisory review of marketing; sales and marketing campaigns that use CPNI; customers' "opt-out" approval or non-approval to



use CPNI; or notifications to customers prior to any solicitation for customer approval to use or disclose CPNI.

PTS will maintain a record of any customer complaints related to their handling of CPNI, and records of PTS' handling of such complaints, for at least two years. The CPNI Compliance Officer will assure that all complaints are reviewed and that PTS considers any necessary changes to its policies or practices to address the concerns raised by such complaints.

PTS will have an authorized corporate officer, as an agent of the company, sign a compliance certificate on an annual basis stating that the officer has personal knowledge that PTS has established operating procedures that are adequate to ensure its compliance with FCC's CPNI rules. The certificate for each year will be filed with the FCC Enforcement Bureau in EB Docket No. 06-36 by March 1 of the subsequent year, and will be accompanied by a summary or copy of this policy that explains how PTS' operating procedures ensure that it is in compliance with the FCC's CPNI rules. In addition, the filing must include an explanation of any actions taken against data brokers and a summary of all customer complaints received in the past year concerning the unauthorized release of CPNI.

## **V. TRAINING**

All employees with access to CPNI receive a summary of PTS' CPNI policies and are informed that (i) any use or disclosure of CPNI or other act or omission not in compliance with such policies will result in disciplinary action, including the termination of employment where appropriate, (ii) proprietary information PTS receives from another carrier for purposes of providing a telecommunications service may be used only for such purpose; and (iii) employees who knowingly facilitate the unauthorized disclosure of CPNI may be subject to criminal penalties.